Self-service Privilege Escalation for Authenticated Users

High **m1k1o** published **GHSA-2gw9-c2r2-f5qf** 2 days ago

Package

Neko

Affected versions

3.0.0 - 3.0.10, 3.1.0, 3.1.1

Patched versions

3.0.11, 3.1.2

Description

Impact

Any authenticated user can immediately obtain full administrative control of the entire Neko instance (member management, room settings, broadcast control, session termination, etc.). This results in a complete compromise of the instance.

Patches

The vulnerability has been patched in the following releases:

- v3.0.11 (backport release)
- v3.1.2 (latest stable release)

Users should upgrade to v3.0.11 or later (for the 3.0 branch) or v3.1.2 or later.

Workarounds

If upgrading is not immediately possible, the following mitigations can reduce risk:

- Restrict access to trusted users only (avoid granting accounts to untrusted parties)
- Run the instance only when needed; avoid leaving it continuously exposed
- Disable or restrict access to the `/api/profile` endpoint if feasible
- Monitor for suspicious privilege changes or unexpected administrative actions

Note: These are temporary mitigations and do not fully eliminate the vulnerability. Upgrading is strongly recommended.

Credits

Thanks to **@blitzkrieg-patch** for responsibly disclosing this vulnerability and reaching out directly. This contribution helped strengthen the project, and the whole community benefits from it.

Severity

High 8.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-39386

Weaknesses

- CWE-20
- CWE-269
- CWE-284
- CWE-639
- CWE-862

Credits

blitzkrieg-patch Finder